

# Benchmarks and Security Tools »»

Clint Kreitner

# Information Security:

- People
- Process
- Technology

# Security Controls (NIST Pub 800-53)

## ■ Management Controls

- Controls that address the security management aspects of the IT system and the management of risk for the system

## ■ Operational Controls

- Controls that address the security mechanisms primarily implemented and executed by people (as opposed to systems)

## ■ Technical Controls

- Controls that address security mechanisms **contained in and executed** by the computer system

*“Through 2005, 90 percent of cyber attacks will continue to exploit known security flaws for which a patch is available or a preventive measure known.”*

» Gartner Group, May 6, 2002

## Most vulnerabilities being exploited by attackers exist because of:

- Software defects
  - Fixed with vendor patches/updates
- Inadequate technical security controls
  - Security settings that enable or disable security features of the OS software

## Examples of security requirements/policies activated via technical controls

- Password length, complexity
- Account lockout after X attempts
- Log what system events?
- Idle time before workstation logoff
- Who is allowed to install printer drivers?
- What unneeded services to disable?

## Example: an ISO Standard 17799 requirement

### ***9.3.2 Unattended user equipment***

Users should ensure that unattended equipment has appropriate protection. Equipment installed in user areas, e.g. workstations or file servers, may require specific protection from unauthorized access when left unattended for an extended period. All users and contractors should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to:

a) terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;

Operating system software includes security parameters that automatically implements a requirement like this when set to a desired value

- **MS Windows** – Amount of Idle Time Before Disconnecting Session
- **Sun Solaris** – Set Default Locking Screensaver Timeout

# Implementing this ISO 17799 requirement on Sun Solaris workstations

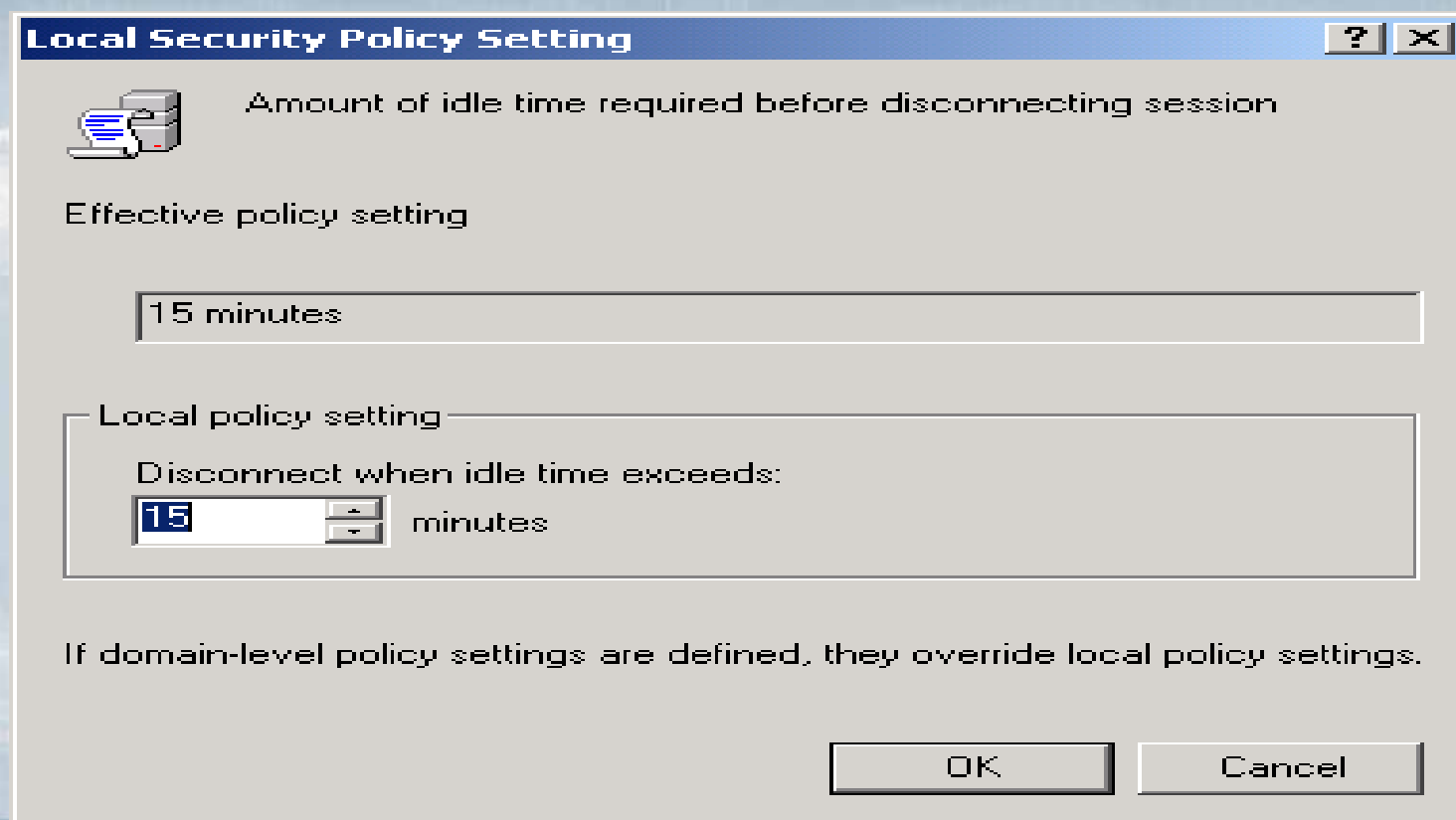
## ***7.7 Set default locking screensaver timeout***

### **Action:**

```
for file in /usr/dt/config/*/sys.resources; do
    dir=`dirname $file` | sed s/usr/etc/
    mkdir -p $dir
    echo 'dtsession*saverTimeout: 10' >>$dir/sys.resources
    echo 'dtsession*lockTimeout: 10' >>$dir/sys.resources
done
```

(The above sequence of commands will cause an idle Solaris workstation to be logged out after 10 minutes)

# Implementing this ISO requirement on a Windows 2000/XP workstation



## Prevailing practice

- Vendors have been shipping unsecured systems with security disabled by default
- Users don't have the knowledge or time to properly secure them
- SysAdmins assuming that vendor default security configurations are adequate
- IS guidance that doesn't go into enough detail

## Why are vendors shipping unsecured systems?

- “Our customers want features and performance. When they want security, we’ll deliver it.”
- “Every customer wants something different. We can’t be expected to deliver and maintain thousands of different configurations.”

## Recognizing the challenge

- Cosmos Club meeting of IT industry leaders in Aug 2000
- Agreed to develop and proliferate detailed operational technical control benchmarks and tools on a collaborative basis

# The Center for Internet Security (CIS)

- Formed in October 2000
- Modeled after other community initiatives, e.g., transportation safety
- A not-for-profit consortium of users
- Focused on the common needs of the global Internet community
- Convenes and facilitates consensus teams that develop detailed operational best practices

## Some of the participants in the consensus effort:

### Government:

- National Institute of Standards and Technology
- Infocomm Development Authority of Singapore
- Naval Surface Warfare Center
- US Treasury Financial Management Service
- Washington State Dept. of Health
- US Army Corps of Engineers
- Defense Info Sys Agency
- Federal Reserve System
- State of Maryland
- NASA
- Australian Nat'l Audit Ofc
- US Dept of Justice
- Library of Congress
- Royal Canadian Mounted Police
- Communications Security Establishment (Canada)
- Canadian CERT
- GSA
- NSA
- DHS
- US CERT

## Participants (cont'd):

### Commercial:

- Eastman Kodak
- Pacific Gas & Electric
- SASKTel
- Lucent Technologies
- LG&E Energy
- Hallmark
- Chevron
- Intel
- Vulcan Materials
- Pfizer
- Caterpillar
- Intuit
- NCR
- Batelle
- Allegheny Energy
- Baltimore Gas & Electric
- Pitney Bowes
- Component Graphics
- Fidelity Nat'l Financial
- Emprise Technologies
- REDW Technologies
- Educational Testing Svc.
- Financial Models Co.
- Agilent Technologies
- Shell Info. Tech. Int'l
- PeopleSoft
- News Corporation
- Anadarko Petroleum

## Participants (cont'd):

### Finance/Insurance/Healthcare

- VISA
- Allstate
- First Union Corporation
- Nat'l Life Assurance Co of Canada
- U.S. Central Credit Union
- Union Bank of California
- City National Bank (LA)
- Swiss Reinsurance Co (SwissRe)
- BMO Financial Group (Canada)
- Fidelity National Financial
- Baylor College of Medicine
- Hospital Corporation of America

### Consulting/Service:

- Symantec
- ISS
- TDS (Germany)
- Data Networks
- Procinct Security
- Sequation
- Grant Thornton
- Investec (UK)
- Belarc
- Polivec

## Participants (cont'd):

### Universities:

- Institute for Security Technology Studies at Dartmouth
- Virginia Tech
- Monash University (Australia)
- University of Alabama at Birmingham
- University of Missouri
- Blenkinge Inst. of Technology (Sweden)
- Utah State University
- University of California, SF
- New York University

### Consulting/Service:

- IBM Consulting
- Deloitte Touche
- Above Security
- BindView
- Harris
- NetIQ
- ConfigureSoft
- SecureNet Solutions
- Computer Sciences Corp.
- Solutionary

## Auditing Participants

- Institute of Internal Auditors (IIA)
- American Institute of Certified Public Accountants (AICPA)
- Information Systems Audit and Control Association (ISACA)

## The consensus process

- Teams are formed with security experts from member organizations
- An initial benchmark draft is obtained or developed
- Consensus is established via email and conference call discussion
- A scoring (compliance checking) tool is developed
- They are made available free to all users globally via the CIS website  
([www.cisecurity.org](http://www.cisecurity.org))

What has collaboration among the participants achieved so far?

## Currently available:

- **Level I Configuration Benchmarks**
  - **Solaris**
  - **Linux**
  - **HP-UX**
  - **Windows NT**
  - **Windows 2000 Professional**
  - **Windows 2000 Server**
  - **Windows XP Professional**
  - **Cisco Router IOS**
  - **Oracle Database**
  - **FreeBSD**

## A Level I Benchmark:

- Can be implemented by a sysadmin of any level of security expertise
- Can be monitored by a compliance tool
- Is not likely to “break” any function
- Represents a baseline level of security

## Currently available:

- Level II Benchmarks
  - Windows 2000 Professional
  - Windows 2000 Server
  - Windows XP Professional (multiple levels)
  - CISCO Router IOS
  - Oracle

## Currently available:

- Configuration Scoring Tools
  - Solaris
  - Linux
  - HP-UX
  - Windows NT
  - Windows 2000 Server
  - Windows 2000 Professional
  - Windows XP
  - Cisco Router IOS
  - Oracle

# THE CENTER FOR INTERNET SECURITY<sup>SM</sup>

Computer: CLINT-NFV6O559O

OVERALL SCORE: 8.5

Scan Time: 08/19/2002 22:10:46

## Scoring

**SCORE**

Select Security Template:

Win2kProGold\_R1.2.inf

☒ Force Gold Standard Scoring  
(Win2K Professional ONLY)

## HFNetChk Options

☐ Use Local HFNetChk Database.

mssecure.xml

☐ Do not evaluate file checksum.☐ Do not perform registry checks.☐ Verbose output.

## Compliance Verification

INF File Comparison Utility

## Group Policy - Domain Users Only

Export Effective Group Policy

## Reporting

Summary Report

Hotfix Report

User Report

Service Report

Scan Log

Debug Log

## Service Packs and Hotfixes

Service Pack Level:

3

Score:

1.25

Hotfixes Missing:

0

Score:

1.25

## Account and Audit Policies

Passwords over 90 Days:

2

Score:

0

Policy Mismatches:

0

Score:

0.8333

Event Log Mismatches:

0

Score:

0.8333

## Security Settings

Restrict Anonymous:

2

Score:

1.25

Security Options Mismatches:

0

Score:

1.25

## Additional Security Protection

Available Services Mismatches:

0

Score:

0.625

User Rights Mismatches:

0

Score:

0.625

NoLMHash:

NTFS:

0

Score:

0.625

Registry and File Permissions:

12

Score:

0

## Under development:

- Benchmarks and Scoring Tools for:
  - Apache Web Server
  - Windows 2003 Server Domain Controller
  - Windows 2003 Server Member Server
  - Cisco PIX Firewall
  - Apple OS X
  - AIX
  - Exchange 2003
  - Juniper Router
  - VoIP
  - Wireless
  - Cisco CatOS
  - and others

## Coming later:

- Applications
- Appliances
- Common combinations of OS, middleware, and applications

Vendors are fully engaged as team members,  
working alongside government and private  
sector users

- Microsoft
- Sun
- HP
- Cisco
- Oracle
- AOL

## The impact...

Case studies show that 80-90% of known vulnerabilities are blocked by the security settings in the consensus benchmarks.....

## Case Study Methodology

- (1) Scan a system “out of the box” and list identified vulnerabilities
- (2) Configure the system with the appropriate benchmark
- (3) Rescan the system and note the vulnerabilities remaining

# Vulnerability Assessment Case studies

<u>Study</u>	<u>System</u>	<u>Benchmark</u>	<u>% of Vuls Eliminated</u>
Solutionary	W2K Server	Level I	<b>85</b>
Citadel	W2K Pro	Level I	<b>81</b>
NSA	W2K Pro	Level II	<b>91</b>
Mitre	W2K Pro	Level II	<b>83 (CVE)</b>
Citadel	W2K Server	Level II	<b>99</b>
Citadel	RedHatLinux	Level I	<b>100</b>

## IA Newsletter describing the NSA and Mitre studies

- Vol 5, Number 3, Fall 2002

[http://iac.dtic.mil/iatac/IA\\_newsletter.html/](http://iac.dtic.mil/iatac/IA_newsletter.html/)

## High payoff things to do right now

- Formally adopt a configuration standard for your various systems and monitor compliance
- Make sure your system purchases require the consensus benchmark settings as vendor installed defaults
- Continuing diligent attention to firewall, anti-virus, software update, and email practice

## Finally...

- Cybersecurity is a comprehensive challenge
- Work the near-term and long-term concurrently
- It's about people, process and technology, so balance your energies among these areas
- View it as an opportunity for organizational improvement, not just regulatory compliance

<http://www.cisecurity.org>  
[ckreitner@cisecurity.org](mailto:ckreitner@cisecurity.org)

